

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-020469

(43)Date of publication of application : 21.01.2000

(51)Int.Cl.

G06F 15/00

H04L 9/08

H04L 9/32

(21)Application number : 10-187925

(71)Applicant : NEC CORP

(22)Date of filing : 02.07.1998

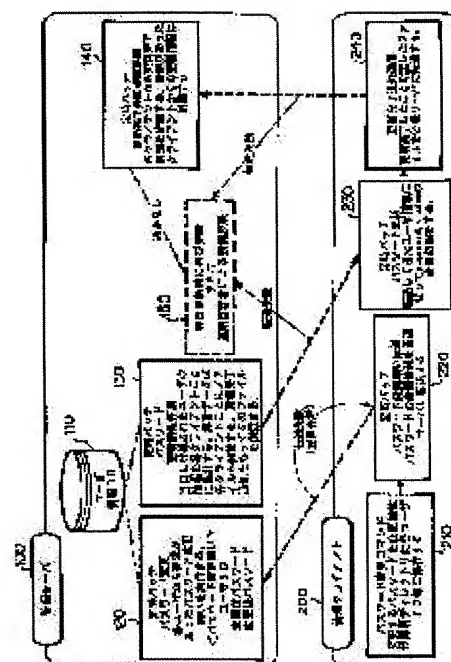
(72)Inventor : FUJIWARA YOHEI

## (54) METHOD AND DEVISE FOR MANAGING PASSWORD

(57)Abstract:

**PROBLEM TO BE SOLVED:** To improve the security of NIS of a UNIX system and to reduce the burden imposed on a managing server.

**SOLUTION:** Concerning the password managing method for managing a password for permitting the use of data in a network for a user, the method is provided with a managing client 200 for managing the user, a managing server 100 for managing the passwords of all the uses through the respective managing clients 200, and the user information data base for storing the password information of users to be used of the respective managing clients 200. When a user is to update the password, the user inputs the new password to the managing client 200, the managing client 200 stores the former enciphered password and the new enciphered password in pair to the password change request file at fixed time and transfers both the enciphered passwords to the managing server 100, and the managing server 100 performs processing for changing the password of the user while referring to the said user information data base at fixed time.



\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.\*\*\*\* shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

## CLAIMS

---

[Claim(s)]

[Claim 1]When it has the following and a user updates a password, a user inputs a new password into said management client, Said management client stores the old encrypted password and a new encrypted password in a file for a password change wish on schedule at a pair, . Both encrypted passwords are transmitted to said managing server, and it is characterized by said managing server performing processing which changes a user's change password referring to said user information data base on schedule. A password management method which manages a password for permitting data use in a user's network.

A management client which manages a user.

A managing server which manages All Users's password through said each management client.

A user information data base which stores a user's password information used by said each management client.

[Claim 2]A password management method, wherein said each management client and said managing server perform said password change processing by regular batch processing on schedule in the password management method according to claim 1.

[Claim 3]A password management method which manages a password for permitting data use in a user's network, comprising:

A step which sets up one server which performs password management.

In a step which makes other machines a management client, and said each management client, A step which performs processing which is not immediately reflected in a system when there is a password change demand by a user, A step which saves password change information per user ID to a password management directory, if on schedule comes -- a managing server from said each management client -- a password -- changing -- with a step to transmit. A step which will process a password change wish transmitted from said each management client, and will check that the password change wish concerned is effective if said managing server side also becomes on schedule, A step which change of a password completes by processing password update information transmitted from said managing server in said each management client when said managing server became a step which transmits password update information to said each management client on schedule, and being reflected in said network.

[Claim 4]New password information transmitted between said management client and said managing server in the password management method according to claim 3 is not what was enciphered by standard password management function for OS, A password management method enciphering using a common cryptographic key managed by said managing server and said each management client.

[Claim 5]A password management device which manages a password for permitting data use in a user's network, comprising:

A management client which manages a user.

A managing server which manages All Users's password through said management client.

An input means which is provided with a user information data base which stores a user's

password information used by said each management client and as which, as for said management client, said user inputs a new password into said management client.

A file storage means which stores the old encrypted password and a new encrypted password in a file for a password change wish on schedule at a pair.

A transfer means which transmits said both encrypted passwords to said managing server.

A password change processing means to perform processing changed into said new password of said user a preparation and said managing server referring to said user information data base on schedule.

A transfer means which transmits password information of a result depended on said password change processing means to said management client using said both encrypted passwords and a common encoding means.

[Claim 6] In the password management device according to claim 5, said management client, Encipher, respectively, save an old password and a new password which were inputted by said input means, carry out an encryption new password which enciphered a new password only for management, and an encryption old password which enciphered an old password is made management, A password management device transmitting to said managing server.

---

[Translation done.]

\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention, without using NIS (Network Information Service) generally used in a UNIX system, Improvement in security is aimed at and it is related with the password management method and password management device which perform password management which is used when operating two or more machines, and which was put in block.

[0002]

[Description of the Prior Art]Conventionally, it is indicated by JP,60-164859,A as a password management method. This gazette about the password management method of a distributed processing computer system, As opposed to what had had and managed the password database individually per conventional computer, A local password database is installed in the local computer by which distributed installation was carried out, Share a local computer and to the host computer which carries out central control. The host password database which includes all the local password databases is installed, It is characterized by registering a password into a host password database and the appointed local password database, respectively, and carrying out common management from the arbitrary terminals connected to this system. In this way, the troublesomeness of the move procedure of the user by having managed independently for each [ which was distributed conventionally ] computer of every is removable, Prevention of the unauthorized use of a password could be coped with promptly, and the password registration management function that size is big did not need to be provided for every local, either, and has done so the effect of enabling simplification of the function of a local computer, and mitigation of load.

[0003]A "network user authentication method" is indicated by JP,8-335207,A, and it is in it. The system chart indicated in this gazette is shown and explained to drawing 8. As shown in drawing 8, there are some which access each network mutually via a gateway computer. In order to exploit the resources of such an integrated network, the user needs to prove the justification of his identity to the server which has a user authentication function in each connected network. Calling this operation login, a user provides a password to a server and proves his identity.

[0004]In drawing 8, when a user logs in to the network 1 from the computers 15-16 for users of the network 9, he will pass the gateway computer 11. The security system in such two or more hierarchies' network, It is a method which judges the existence of the access right to other nodes with transmitting the password to each node which the user inputted to the gateway computer 11 of the node used as a direct access point, and a node checking a password.

[0005]The communication media 2 which the network 1 connects each element in the network 1 physically and logically, and turn into a medium of various data transmission, The management computer 3 which performs specially authenticating processing of each element which constitutes the network 1, or a user, The database 4 for managing the information about each element and user of the network 1, including ID, a password, etc., The authentication service part 5 which gives an encryption key and a login certificate to a requiring agency according to the demand from each network element and user, The database manager 6 which performs read-out and the writing of data from the database 4, The server 7 which provides various services

according to the demand from the client 8, It is \*\* constituted with the client 8 which communicates with the management computer 3 or the server 7 according to the demand which provides the user of the network 1 with a command interface or an application program, and is emitted by the user through them.

[0006]The network 9 managed independently [ the network 1 ], The communication media 10 which connect physically between each element in nine in a network, and logically, and turn into a medium of various data transmission, The gateway computer 11 with the role which is connected to the communication media 2 and 10, transmits the command from the computers 15-16 between users to the network 1, and replies a result to the computer for users, The authentication processing part 12 which transmits an authentication demand to the management computer 3, and performs login processing to the network 1, The password management table 13 which manages the information about the user of the gateway computer 11 and the network 9, including ID, a password, etc., It is \*\* constituted with the server 14 which provides various services, the computers 15 and 16 for users which communicate according to a demand of the user of the network 9, and the authentication demand part 17 which enters a user's ID and password.

[0007]Then, if an authentication demand and user ID are transmitted to the management computer 13 from the user's computer 15 in the case of login, the management computer 13 will be returned to the client for which a user uses the login certificate enciphered with the user's password, and an encryption key. The client 8 decrypts a login certificate and an encryption key with the password which the user entered. In this way, attestation is made possible, without a password flowing into the network 1. The user in the network 1 makes attestation possible, without pouring a password to the network 9 similarly, and supposes that the illegal acquisition of the password in a gateway computer can be eliminated.

[0008]On the other hand in the UNIX system which it has as standard, a network function with NFS (Network File System) of a distributed file system. When performing two or more user management of a machine to a package, the so-called NIS (Network Information Service) of the name server is used frequently. Central control of the name of each user on a managing server and a password can be performed without troubling the labor of a network administrator making change of a system reflect for each machine of every by using NIS.

[0009]NIS comprises on a client server model. An NIS server is a host with the NIS data file called a map, and an NIS client is a host who demands such map information.

[0010]

[Problem(s) to be Solved by the Invention]However, there are the following problems in NIS.

[0011]Since others' password is easily decipherable to it once password information is flying about to the 1st continuously and obtains a network top to it like [ when changing the time of logging in, and a password ], I hear that there is a problem in security and it is in it.

[0012]Since it says at a server an inquiry whenever a demand has [ 2nd ] a client, or a map is transmitted to a slave at any time from a server, I hear that load is applied to a network and a managing server, and it is in them. According to the gazette explained by the above-mentioned conventional example, this 2nd problem is not solved.

[0013]This invention improves the security of NIS of the above-mentioned UNIX system, and it makes it a technical problem to ease the burden of a managing server.

[0014]

[Means for Solving the Problem]In a password management method which manages a password for this invention to permit data use in a user's network, A management client which manages a user, and a managing server which manages All Users's password through said each management client, It has a user information data base which stores a user's password information used by said each management client, When a user updates a password, a user inputs a new password into said management client, Said management client stores the old encrypted password and a new encrypted password in a file for a password change wish on schedule at a pair, Processing which changes a user's change password is performed transmitting both encrypted passwords to said managing server, and said managing server referring to said user information data base on schedule.

[0015]In a password management method which manages a password for this invention to permit data use in a user's network, In a step which makes a management client a step which sets up one server which performs password management, and other machines, and said each management client, A step which performs processing which is not immediately reflected in a system when there is a password change demand by a user, A step which saves password change information per user ID to a password management directory, if on schedule comes -- a managing server from said each management client -- a password -- changing -- with a step to transmit. A step which will process a password change wish transmitted from said each management client, and will check that the password change wish concerned is effective if said managing server side also becomes on schedule, A step to which said managing server transmits password update information to said each management client, If on schedule comes, in said each management client, it will be characterized by step which change of a password completes, and a thing, \*\* and others, by processing password update information transmitted from said managing server, and being reflected in said network.

[0016]This invention equips with the following a password management device which manages a password for permitting data use in a user's network.

A management client which manages a user.

A managing server which manages All Users's password through said each management client.

An input means which is provided with a user information data base which stores a user's password information used by said each management client and as which a user inputs a new password into said management client, A file storage means by which said management client stores the old encrypted password and a new encrypted password in a pair on schedule at a file for a password change wish, A password change processing means to perform processing a transfer means which transmits said both encrypted passwords to said managing server, and said managing server change a user's change password referring to said user information data base on schedule.

[0017]

[Embodiment of the Invention]The embodiment by this invention is described in detail, referring to drawings.

[0018][A 1st embodiment]

(Composition of this embodiment) In drawing 1, it becomes the management client 200 of WS (WorkStation) which has adopted UNIX, and the managing server 100 as an operating system that this method is applicable. Although the managing server 100 comprises one set, if the number of the management client 200 is one or more, restriction in particular is not provided.

[0019]The password change processing 120 by the regular batch which performs the password change wish where user information data base DB110 has been arranged, and which had a demand in the managing server 100 from each user, The regular batch password update information creation processing 130 which writes a user's information registered into that day in which total for every client, keep total data to a file for every client, and the file is deleted with an updating completion notification, An updating completion notification is checked from each client, and each processing of the regular batch update completion notification confirming processing 140 in which the update information from a client with a notice is deleted is made. When you have a transfer failure and no notice, updating or the compulsive reflection 150 by an operations manager is again processed on the next day at the time of updating.

[0020]If the password change command 210 which saves the password to change for every user to the directory for changed information registration is emitted by each management client 200, Password change wish transmission 220 which transmits the changed information of a password to a managing server in regular batch is performed, The password update 230 which carries out change processing of password shadow according to User Information transmitted in regular batch is performed, and updating completion notification transmission 240 is performed to a managing server.

[0021]Since the managing server and management client by this embodiment performed updating and management processing of the password, used expression called especially a managing

server and a management client, but. Even if it is a general server and a client, since the composition, and operation and an operation of this embodiment can be attained, it does not adhere to the name.

[0022]With reference to (operation of this embodiment), next drawing 2, operation of this whole embodiment is explained in detail. By a UNIX system, since it is a time of changing a stage and a password at the beginning which registers self name and password when you wish entry to a system when generated by the password in a transmission line, the operation at the time of a password change is explained.

[0023]First, in each management client 200, a user executes the password change command 210 prepared for these methods. The password enciphered from the password entry of each management client (trypt) is extracted (211). The password before the user itself changing into the next is entered (212). Compare this enciphered password with the entered password (213), and user authentication will be ended if in agreement, Enter a new password twice for a check (214), and the file for a password change wish is created, The new password enciphered as the enciphered old password is saved (215), a new password is enciphered, it shall be only for management, the inputted old password is enciphered, and it transmits to (216) and the managing server 100 as an object for management.

[0024]The file for a password change wish is created for every user ID by executing this command. The new password and old password which were enciphered by the exclusive cryptographic key are saved at this file. If this file becomes on schedule every day, it will be transmitted to a managing server (management client password change command 210 of drawing 2).

[0025]Next, with the managing server 100, as shown in drawing 2, if on schedule comes every day, password change processing will be performed (120). The new password which read each transmitted file for a password change wish, and was enciphered as the enciphered old password is read (121). The password of User Information DB110 is compared with the sent old password (122), and if equal, a new password (what was enciphered by the exclusive cryptographic key) is registered into User Information DB110 (123), and is stored (password change processing 120 of the managing server of drawing 2).

[0026]Next, when on schedule comes in the managing server 100 every day, as the user update information creation processing 130, A password change is read from User Information DB110 (161), and the updated list list which bundled up the enciphered password only for [ of an on / User Information DB110 ] management is written in the file for transmission (162). It is transmitted to each management client 200 which corresponds this user update information (163).

[0027]When on schedule comes every day, the transmitted user update information file is read and composite-ized (231), and the password registered on User Information DB110 is made to reflect in a system by each management client 200 finally (management client user information update processing 230 of drawing 2).

[0028]Next, each processing is explained concretely.

[0029]With reference to drawing 4, the password change command 210 prepared for each management client 200 is explained first. If this command is executed, the input of the present password will be required (211) and the present password will be entered (212). If the entered password and the password registered into /etc/shadow are equal (213), the input of a new password will be required twice (214,214'). If a new password is the same twice [ both ] (215), an old password and a new password will be written in a password change wish file (217), and a password will be enciphered by the cryptographic key only for management (218). The enciphered password is transmitted to a managing server. not carrying out password coincidence at Steps 21A and 21B by Step 213,215, on the other hand, in not being equal -- \*\*\*\*\* -- warning [ like ] is emitted and it ends.

[0030]Next, with reference to drawing 5, the password change wish transmission processing 220 is explained. If on schedule comes every day, the password change wish file for every user under a password management directory will be searched with each management client 200 (221), and a password change file will be altogether transmitted to the managing server 100 using the rcp



command (222). It judges whether it succeeded in transmission (223), and the password change wish file on each management client is deleted after checking a transmission success (224). When transmission goes wrong at Step 223, processing again transmitted at the time of next starting is performed.

[0031]Next, with reference to drawing 3, the password change processing 120 on the managing server 100 is explained. In the managing server 100, if on schedule comes every day, the password change wish file 220 transmitted from each management client will be processed. First, the list of files in a password management directory is created, and it processes it one [ at a time ] (121). Next, an old password and a new password are read from the password information file 111 (122). Next, the password on User Information DB110 is read (123). About each file, if the password on User Information DB110 and the old password on a file are equal (124), a new password is made to reflect on User Information DB110, and is stored (125). (status: password change) Otherwise, the E-mail of the purport that it is an abnormal condition is transmitted to a user with a request, and addressing to a managing server operator (128), and status on the user D information B is changed into "password update failure" (129). The transmitted file is deleted after these processings are completed (126). The above-mentioned processing is repeated for every user (127).

[0032]Next, with reference to drawing 6, the user update information creation processing 130 on the managing server 100 is explained. If on schedule comes in the managing server 100 every day, All Users's update information will be checked on User Information DB110 (131), Search a list with a password update and it is judged whether the flag of the purport that it updated is ON (132), Check a using state for every applicable registration destination (133), judge whether status of a using state is a password change or one of the password update failure (134), and if it is a password change, It creates in the form where a user update information file is Append(ed) as a transfer file of an applicable registration destination (135). This is processed for every registration destination, if all the registration destinations are checked (137) and it ends, an update flag will be cleared (138), and it judges whether All Users's check was ended (139), and ends.

[0033]Finally, with reference to drawing 7, the renewal 230 of User Information on the management client 200 is explained. In each management client 200, if on schedule comes every day, it will start as a regular batch and the information transmitted from the managing server 100 once [ 1 ] per day will be processed. The management client 200 searches the transmitted User Information update file (234), processes it sequentially according to the contents of a user update information file, and is read from the pointer of a file by one line (235). Next, setting out of a management client is changed into the password shown from the managing server 100 (236). The additional writing of the updating result is carried out at an updated information file (237). Next it confirms whether reading was ended to the last of a user update information file (238), and an updated information file is transmitted to a managing server (239). In this way, if change of a password is checked, it will be written in an updated information file and an updated information file will be transmitted to a managing server after completing all the processings (239).

[0034]As mentioned above, in drawing 1 the management client 200, In order to update a password on schedule as regular batch processing, change processing of a password is performed according to transmitted User Information (230), and the file which described having carried out the completion of updating of this result for updating completion notification transmission is transmitted to the managing server 100 (240). In a managing server, an updating completion notification is checked from each management client 200 as updating completion notification confirming processing of regular batch processing. Then, the update information from a management client with a notice is deleted. In this way, a series of batch processing is ended (140). here, when transmission goes wrong, in the managing server 100, regular batch processing should do, for example to the next day -- it is -- or it is based on an operations manager -- re transfer directions are carried out compulsorily at a management client, and updating completion processing is performed (150).

[0035]



[Effect of the Invention]According to this invention, since password information was enciphered and it has transmitted on a network using a managing server and the cryptographic key for exclusive use which each management client shared and has been managed, it is in being easily undecipherable even if the password information file under transmission includes others' hand. As a result, the security of a system improves.

[0036]Since central control is carried out on a managing server, the batch management of the management client which are two or more UNIX machines can be carried out. As a result, the labor in a system management reduces.

[0037]Since information transfer between a managing server and each management client is performed not on time one but every day using a regular batch, the traffic which flows on a network can be reduced and the load of a managing server and each management client can be reduced. As a result, the load to a network is reduced.

---

[Translation done.]

\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.\*\*\* shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1]It is a schematic diagram of the password management function by the embodiment of this invention.

[Drawing 2]It is a flow chart of the password management by the embodiment of this invention.

[Drawing 3]It is a flow chart of password change processing of the managing server by the embodiment of this invention.

[Drawing 4]It is a flow chart of the password change command processing of the management client by the embodiment of this invention.

[Drawing 5]It is a flow chart of password change wish transmission processing of the management client by the embodiment of this invention.

[Drawing 6]It is a flow chart of user update information creation processing of the managing server by the embodiment of this invention.

[Drawing 7]It is a flow chart of user update information processing of the management client by the embodiment of this invention.

[Drawing 8]It is a system-outline figure by the conventional network authentication method.

[Description of Notations]

100 Managing server

110 User information data base

120 Regular batch password change processing

130 Regular batch password processing

140 Regular batch update completion notification confirming processing

200 Management client

210 Password change command

220 Regular batch password change wish transmission processing

230 Regular batch password update processing

240 Updating completion notification check

---

[Translation done.]



## 【特許請求の範囲】

【請求項 1】 ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、

ユーザを管理する管理クライアントと、前記各管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、

ユーザがパスワードを更新する際、ユーザは新パスワードを前記管理クライアントに入力し、前記管理クライアントは定時にパスワード変更願い用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納し、両暗号化パスワードを前記管理サーバに転送し、前記管理サーバは定時に前記ユーザ情報データベースを参照しつつユーザの変更パスワードを変更する処理を行うことを特徴とするパスワード管理方法。

【請求項 2】 請求項 1 に記載のパスワード管理方法において、前記各管理クライアント及び前記管理サーバは、定時に定時バッチ処理により前記パスワード変更処理を行うことを特徴とするパスワード管理方法。

【請求項 3】 ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、

パスワード管理を行うサーバを一台設定するステップと、

他のマシンは管理クライアントとするステップと、

前記各管理クライアントにおいて、ユーザによりパスワード変更要求があったときシステムにすぐ反映しない処理を行うステップと、

パスワード管理ディレクトリにユーザ ID 単位にパスワード変更情報を保存するステップと、

定時になると前記各管理クライアントから管理サーバにパスワードの変更願いが転送するステップと、

前記管理サーバ側も定時になると前記各管理クライアントから転送されてきたパスワード変更願いを処理して当該パスワード変更願いが有効であることを確認するステップと、

前記管理サーバが前記各管理クライアントに対してパスワード更新情報を転送するステップと、

定時になると前記各管理クライアントでは前記管理サーバから転送されたパスワード更新情報を処理し前記ネットワークに反映することによりパスワードの変更が完了するステップと、からなることを特徴とするパスワード管理方法。

【請求項 4】 請求項 3 に記載のパスワード管理方法において、

前記管理クライアントと前記管理サーバ間で転送される新パスワード情報は OS 標準のパスワード管理機能により暗号化されたものではなくて、前記管理サーバ及び前

記各管理クライアントで管理している共通の暗号化キーを用いて暗号化したものであることを特徴とするパスワード管理方法。

【請求項 5】 ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理装置において、

ユーザを管理する管理クライアントと、前記管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、

前記管理クライアントは、前記ユーザは新パスワードを前記管理クライアントに入力する入力手段と、

定時にパスワード変更願い用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納するファイル記憶手段と、

前記両暗号化パスワードを前記管理サーバに転送する転送手段と、を備え、

前記管理サーバは、定時に前記ユーザ情報データベースを参照しつつ前記ユーザの前記新パスワードに変更する処理を行うパスワード変更処理手段と、

前記パスワード変更処理手段による結果のパスワード情報を前記両暗号化パスワードと共通の暗号化手段を用いて前記管理クライアントに転送する転送手段と、を備えたことを特徴とするパスワード管理装置。

【請求項 6】 請求項 5 に記載のパスワード管理装置において、

前記管理クライアントは、前記入力手段で入力した旧パスワードと新パスワードとをそれぞれ暗号化して保存し、

新パスワードを暗号化した暗号化新パスワードを管理専用とし、旧パスワードを暗号化した暗号化旧パスワードを管理用として、前記管理サーバに転送することを特徴とするパスワード管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、UNIX システムにおいて、一般に利用されているNIS (Network Information Service) を使用せずに、セキュリティの向上を図り、複数マシンを操作する際に用いる一括したパスワード管理を行うパスワード管理方法及びパスワード管理装置に関する。

【0002】

【従来の技術】従来、パスワード管理方式として、特開昭 60-164859 号公報に開示されている。本公報は、分散処理コンピュータシステムでのパスワード管理方式に関し、従来のコンピュータ単位で個別にパスワードデータベースを有して管理していたものに対し、分散設置されたローカルコンピュータにローカルパスワードデータベースを設置し、ローカルコンピュータを共有し、集中管理するホストコンピュータに、全てのローカルパ

スワードデータベースを包括するホストパスワードデータベースを設置し、該システムに接続される任意の端末よりパスワードをホストパスワードデータベースならびに指定のローカルパスワードデータベースにそれぞれ登録し、共通管理することを特徴としている。こうして、従来分散した各コンピュータ毎に別々に管理していたことによる使用者の移動手続の煩わしさを除去でき、パスワードの不正使用の防止に迅速に対処でき、サイズの大きなパスワード登録管理機能も、ローカル毎に具備する必要もなく、ローカルコンピュータの機能の簡素化と負荷の軽減を可能とするという効果を奏している。

【0003】また、特開平8-335207号公報に「ネットワークユーザ認証方法」が開示されている。図8に該公報に記載されたシステム図を示して説明する。図8に示すように、ゲートウェイコンピュータを介して各ネットワークを相互にアクセスするものがある。このような統合ネットワークの資源を利用するために、ユーザは接続された各ネットワーク中のユーザ認証機能を有するサーバに対して自分の身元の正当性を証明する必要がある。この動作をログインと呼び、ユーザはサーバに対してパスワードを提供して自分の身元を証明する。

【0004】図8において、ユーザはネットワーク9のユーザ用コンピュータ15～16からネットワーク1へログインする際に、ゲートウェイコンピュータ11を介することとなる。このような2階層以上のネットワークにおけるセキュリティ方式は、ユーザが入力した各ノードへのパスワードを、直接のアクセス先となるノードのゲートウェイコンピュータ11に送信し、ノードがパスワードをチェックすることで他のノードへのアクセス権の有無を判断する方式である。

【0005】ネットワーク1は、ネットワーク1内の各要素を物理的・論理的に接続し各種データ転送の媒体となる通信媒体2と、ネットワーク1を構成する各要素やユーザの認証処理を専門に行う管理コンピュータ3と、ネットワーク1の各要素やユーザに関する情報（ID、パスワード等）を管理するためのデータベース4と、ネットワークの各要素やユーザからの要求に応じて暗号鍵やログイン証明書を要求元に与える認証サービス部5と、データベース4からデータの読み出しや書き込みを行うデータベース管理部6と、クライアント8からの要求に応じて各種サービスを提供するサーバ7と、ネットワーク1のユーザにコマンドインターフェースやアプリケーションプログラムを提供しそれらを通じてユーザから発せられる要求に応じて管理コンピュータ3やサーバ7と通信を行うクライアント8と、から構成されている。

【0006】また、ネットワーク1とは独立に管理されるネットワーク9は、ネットワーク内9内の各要素間の物理的・論理的に接続し各種データ転送の媒体となる通信媒体10と、通信媒体2と10に接続されユーザ間コ

ンピュータ15～16からのコマンドをネットワーク1に送信し結果をユーザ用コンピュータに返信する役割をもつゲートウェイコンピュータ11と、管理コンピュータ3に認証要求を送信してネットワーク1へのログイン処理を行う認証処理部12と、ゲートウェイコンピュータ11及びネットワーク9のユーザに関する情報（ID、パスワード等）を管理するパスワード管理テーブル13と、各種サービスを提供するサーバ14と、ネットワーク9のユーザの要求に応じて通信するユーザ用コンピュータ15、16と、ユーザのIDやパスワードを入力する認証要求部17と、から構成されている。

【0007】そうして、ログインの際、ユーザ用コンピュータ15から管理コンピュータ13に認証要求とユーザIDを送信すると、管理コンピュータ13はユーザのパスワードで暗号化したログイン証明書と暗号鍵をユーザが使用するクライアントに返す。クライアント8はユーザが入力したパスワードによりログイン証明書と暗号鍵を復号化する。こうして、ネットワーク1にはパスワードが流れずに認証を可能とする。また、ネットワーク1内のユーザは、同様にネットワーク9にパスワードを流さずに認証を可能とし、ゲートウェイコンピュータにおけるパスワードの不正入手を排除できるとしている。

【0008】また一方、ネットワーク機能を標準で備えるUNIXシステムにおいて、分散ファイルシステムのNFS（Network File System）と共に、複数マシンのユーザ管理を一括に行う際にはいわゆる名前サーバのNIS（Network Information Service）が頻繁に使用されている。NISを使用することにより、ネットワーク管理者は個々のマシン毎にシステムの変更を反映させるといった労力を煩わせることなく、管理サーバ上での各ユーザの名前とパスワードとの集中管理が行える。

【0009】NISはクライアント・サーバモデル上で構成される。NISサーバとは、マップと呼ばれるNISデータファイルを持つホストのことで、NISクライアントとは、これらのマップ情報を要求するホストのことである。

【0010】

【発明が解決しようとする課題】しかし、NISには、次のような問題点がある。

【0011】第1に、ログインする際やパスワードを変更するときのように、パスワード情報がネットワーク上を絶えず飛び交っており、いったん入手すれば他人のパスワードを容易に解読出来るので、セキュリティに問題があるということである。

【0012】また、第2に、クライアントが要求のある度にサーバに問い合わせにいたり、サーバからスレーブにマップが随時転送されるので、ネットワーク、管理サーバに負荷がかかるということである。上述の従来例で説明した公報によれば、この第2の問題点を解決していない。

【0013】本発明は、上記UNIXシステムのNISのセキュリティを向上すると共に、管理サーバの負担を軽減することを課題とする。

【0014】

【課題を解決するための手段】本発明は、ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、ユーザを管理する管理クライアントと、前記各管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、ユーザがパスワードを更新する際、ユーザは新パスワードを前記管理クライアントに入力し、前記管理クライアントは定時にパスワード変更願用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納し、両暗号化パスワードを前記管理サーバに転送し、前記管理サーバは定時に前記ユーザ情報データベースを参照しつつユーザの変更パスワードを変更する処理を行うことを特徴とする。

【0015】また、本発明は、ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、パスワード管理を行うサーバを一台設定するステップと、他のマシンは管理クライアントとするステップと、前記各管理クライアントにおいて、ユーザによりパスワード変更要求があったときシステムにすぐ反映しない処理を行うステップと、パスワード管理ディレクトリにユーザID単位にパスワード変更情報を保存するステップと、定時になると前記各管理クライアントから管理サーバにパスワードの変更願いが転送するステップと、前記管理サーバ側も定時になると前記各管理クライアントから転送されてきたパスワード変更願いを処理して当該パスワード変更願いが有効であることを確認するステップと、前記管理サーバが前記各管理クライアントに対してパスワード更新情報を転送するステップと、定時になると前記各管理クライアントでは前記管理サーバから転送されたパスワード更新情報を処理し前記ネットワークに反映することによりパスワードの変更が完了するステップと、からなることを特徴とする。

【0016】更に、本発明は、ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理装置において、ユーザを管理する管理クライアントと、前記各管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、ユーザは新パスワードを前記管理クライアントに入力する入力手段と、前記管理クライアントは定時にパスワード変更願用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納するファイル記憶手段と、前記両暗号化パスワード

を前記管理サーバに転送する転送手段と、前記管理サーバは定時に前記ユーザ情報データベースを参照しつつユーザの変更パスワードを変更する処理を行うパスワード変更処理手段と、を備えたことを特徴とする。

【0017】

【発明の実施の形態】本発明による実施形態について、図面を参照しつつ詳細に説明する。

【0018】〔第1の実施形態〕

（本実施形態の構成）図1において、本方式を適用できるのはオペレーティングシステムとして、UNIXを採用しているWS（WorkStation）の管理クライアント200と、管理サーバ100となる。管理サーバ100は一台から構成されるが、管理クライアント200の台数は1以上であれば、制限は特に設けていない。

【0019】管理サーバ100には、ユーザ情報データベースDB110が配置され、各ユーザから要求があったパスワード変更願いを実行する定時バッチによるパスワード変更処理120と、当日に登録されたユーザの情報を書くクライアントごとに集計し、集計データは各クライアント毎にファイルへ保管し、更新完了通知をもってそのファイルを削除する定時バッチパスワード更新情報作成処理130と、各クライアントから更新完了通知を確認し、通知があったクライアントからの更新情報は削除する定時バッチ更新完了通知確認処理140の各処理がなされる。また、転送失敗や通知なしの場合に翌日更新時に再び更新又は運用管理者による強制反映150の処理を行う。

【0020】また、各管理クライアント200には、変更するパスワードを変更情報登録用ディレクトリに各ユーザ毎に保存するパスワード変更コマンド210が発せられると、定時バッチでパスワードの変更情報を管理サーバに転送するパスワード変更願い転送220が実行され、定時バッチで転送してきたユーザ情報に従ってpassword shadowの変更処理をするパスワード更新230が実行され、更新完了通知転送240が管理サーバに対して実行される。

【0021】本実施形態による管理サーバや管理クライアントは、パスワードの更新及び管理処理を実行するので、特に管理サーバや管理クライアントという表現を用いたが、一般のサーバやクライアントであっても、本実施形態の構成及び動作・作用を達成できるので、その名称に拘ることはない。

【0022】（本実施形態の動作）次に、図2を参照して、本実施形態の全体の動作について詳細に説明する。UNIX系システムでは、パスワードが伝送ラインに発生する場合は、システムへの参入を希望するときの自己の名前とパスワードを登録する当初段階と、パスワードを変更するときであるので、パスワード変更時における動作について説明する。

【0023】まず、各管理クライアント200におい

て、ユーザが、本方式用に用意されたパスワード変更コマンド 210 を実行する。各管理クライアントのパスワードエントリから暗号化 (trypt) されたパスワードを抽出する (211)。つぎに、ユーザ自身が変更前のパスワードを入力する (212)。この暗号化されたパスワードと入力したパスワードとを比較し (213)、一致しておればユーザ確認を終了して、新しいパスワードを確認のため 2 回入力し (214)、パスワード変更願用ファイルを作成し、暗号化した旧パスワードと暗号化した新パスワードとを保存し (215)、新パスワードを暗号化して管理専用とし、入力した旧パスワードを暗号化して管理用として (216)、管理サーバ 100 に転送する。

【0024】このコマンドを実行することによりパスワード変更願用ファイルがユーザ ID 毎に作成される。このファイルには専用暗号化キーで暗号化された新パスワードと旧パスワードが保存される。このファイルは毎日定時になると管理サーバに転送される (図 2 の管理クライアント・パスワード変更コマンド 210)。

【0025】次に、図 2 に示すように、管理サーバ 100 では毎日定時になると、パスワード変更処理を実行する (120)。転送されてきた各パスワード変更願用ファイルを読み込み、暗号化された旧パスワードと暗号化された新パスワードとを読み込み (121)、ユーザ情報 DB 110 のパスワードと送られてきた旧パスワードを比較し (122)、等しければ新パスワード (専用暗号化キーで暗号化されたもの) をユーザ情報 DB 110 に登録して (123)、格納する (図 2 の管理サーバのパスワード変更処理 120)。

【0026】次に、管理サーバ 100 では毎日定時になると、ユーザ更新情報作成処理 130 として、ユーザ情報 DB 110 からパスワード変更を読み込み (161)、ユーザ情報 DB 110 上の管理専用の暗号化されたパスワードを一括した更新されたリスト一覧を転送用ファイルに書き込む (162)。このユーザ更新情報を該当する各管理クライアント 200 へ転送される (163)。

【0027】最後に、各管理クライアント 200 では毎日定時になると、転送されてきたユーザ更新情報ファイルを読み込み、複合化して (231)、ユーザ情報 DB 110 上に登録されているパスワードをシステムに反映させる (図 2 の管理クライアントユーザ情報更新処理 230)。

【0028】次に、各処理について具体的に説明する。

【0029】まず図 4 を参照して、各管理クライアント 200 に用意するパスワード変更コマンド 210 について説明する。このコマンドを実行すると、現在のパスワードの入力を要求され (211)、現在のパスワードを入力する (212)。入力したパスワードと /etc/shadow に登録されているパスワードが等しければ (21

3)、新しいパスワードの入力が 2 回要求される (214, 214')。新しいパスワードが 2 回共に同じであれば (215)、パスワード変更願用ファイルに旧パスワードと新パスワードが書き込まれ (217)、パスワードは管理専用暗号化キーで暗号化する (218)。暗号化されたパスワードは管理サーバに転送される。一方、ステップ 213, 215 で等しくない場合には、ステップ 21A, 21B で、パスワード一致せずというような警告を発して終了する。

【0030】次に、図 5 を参照して、パスワード変更願用転送処理 220 について説明する。毎日定時になると、各管理クライアント 200 ではパスワード管理ディレクトリ下にあるユーザ毎のパスワード変更願用ファイルを検索し (221)、パスワード変更ファイルを全て rcp コマンドを用いて管理サーバ 100 に転送する (222)。転送に成功したか否かを判断し (223)、転送成功を確認後、各管理クライアント上のパスワード変更願用ファイルを削除する (224)。ステップ 223 で転送に失敗した場合には、次の起動時に再度転送する処理を行う。

【0031】次に、図 3 を参照して、管理サーバ 100 上でのパスワード変更処理 120 について説明する。管理サーバ 100 では、毎日定時になると、各管理クライアントから転送されてきたパスワード変更願用ファイル 220 を処理する。まず、パスワード管理ディレクトリにあるファイルのリストを作成し、一つずつ処理する (121)。

つぎに、パスワード情報ファイル 111 から旧パスワードと新パスワードとを読み込む (122)。次にユーザ情報 DB 110 上のパスワードを読み込む (123)。各ファイルについて、ユーザ情報 DB 110 上のパスワードとファイル上の旧パスワードが等しければ (124)、新パスワードをユーザ情報 DB 110 上に反映させて (status: パスワード変更) 格納する (125)。そうでなければ依頼のあったユーザと管理サーバオペレータ宛に異常状態である旨の電子メールを送信し (128)、ユーザ D 情報 B 上の status を「パスワード更新失敗」に変更する (129)。これらの処理が終了した後に、転送されてきたファイルを削除する (126)。各ユーザ毎に上記処理を繰り返す (127)。

【0032】次に図 6 を参照して、管理サーバ 100 上でのユーザ更新情報作成処理 130 について説明する。管理サーバ 100 では毎日定時になると、ユーザ情報 DB 110 上で全ユーザの更新情報をチェックし (131)、パスワード更新のあったリストを検索し、更新した旨のフラグが ON であるかどうかを判断し (132)、該当する登録先毎に利用状況をチェックし (133)、利用状況の status がパスワード変更か又はパスワード更新失敗のどれかであるかを判断し (134)、パスワード変更であれば、該当する登録先の転送ファイル



としてユーザ更新情報ファイルをAppendする形で作成する(135)。これを登録先毎に処理し、全登録先をチェックし(137)、終了すれば更新フラグをクリアし(138)、全ユーザのチェックを終了したかを判断し(139)、終了する。

【0033】最後に、図7を参照して、管理クライアント200上でのユーザ情報更新230について説明する。各管理クライアント200では毎日定時になると、定時バッチとして起動し、1日1回管理サーバ100から転送されてくる情報を処理する。管理クライアント200は、転送されてきたユーザ更新情報ファイルを検索し(234)、ユーザ更新情報ファイルの内容に従って順次処理していき、ファイルのポインタから1行分読み込む(235)。つぎに、管理サーバ100から提示されたパスワードに管理クライアントの設定を変更する(236)。更新結果を更新通知ファイルに追加書き込みする(237)。つぎに、ユーザ更新情報ファイルの最後まで読み込みを終了したかをチェックし(238)、更新通知ファイルを管理サーバに送信する(239)。こうして、パスワードの変更が確認されたら、更新通知ファイルに書き込まれ、全ての処理が終了後、更新通知ファイルは管理サーバに転送される(239)。

【0034】上述したように、図1において、管理クライアント200は、定時バッチ処理として、定時にパスワードを更新するため、転送されてきたユーザ情報に従ってパスワードの変更処理を行い(230)、この結果を更新完了通知送信のため、更新完了したことを記述したファイルを管理サーバ100に転送する(240)。管理サーバでは、定時バッチ処理の更新完了通知確認処理として、各管理クライアント200から更新完了通知を確認する。その後、通知のあった管理クライアントからの更新情報は削除する。こうして一連のバッチ処理を終了する(140)。ここで、転送を失敗したときには、管理サーバ100では、例えば翌日に定時バッチ処理がなされか、または運用管理者による強制的に管理クライアントに再転送指示して更新完了処理を実行する(150)。

【0035】

【発明の効果】本発明によれば、管理サーバ、及び各管理クライアントで共有して管理している専用の暗号化キーを利用して、パスワード情報を暗号化してネットワーク上に転送しているので、転送中のパスワード情報ファ

イルが他人の手に渡っても容易に解読出来ないことにある。この結果、システムのセキュリティが向上する。

【0036】また、管理サーバ上で集中管理するため、複数のUNIXマシンである管理クライアントを一括管理できる。この結果、システム管理における労力が軽減する。

【0037】さらに、管理サーバと各管理クライアント間での情報転送が、オンタイムではなくて、毎日定時バッチを用いて行われるため、ネットワーク上を流れるトラフィックを軽減でき、管理サーバと各管理クライアントの負荷を軽減できる。この結果、ネットワークへの負荷が軽減する。

【図面の簡単な説明】

【図1】本発明の実施形態によるパスワード管理機能の概要図である。

【図2】本発明の実施形態によるパスワード管理の流れ図である。

【図3】本発明の実施形態による管理サーバのパスワード変更処理のフローチャートである。

【図4】本発明の実施形態による管理クライアントのパスワード変更コマンド処理のフローチャートである。

【図5】本発明の実施形態による管理クライアントのパスワード変更願い転送処理のフローチャートである。

【図6】本発明の実施形態による管理サーバのユーザ更新情報作成処理のフローチャートである。

【図7】本発明の実施形態による管理クライアントのユーザ更新情報処理のフローチャートである。

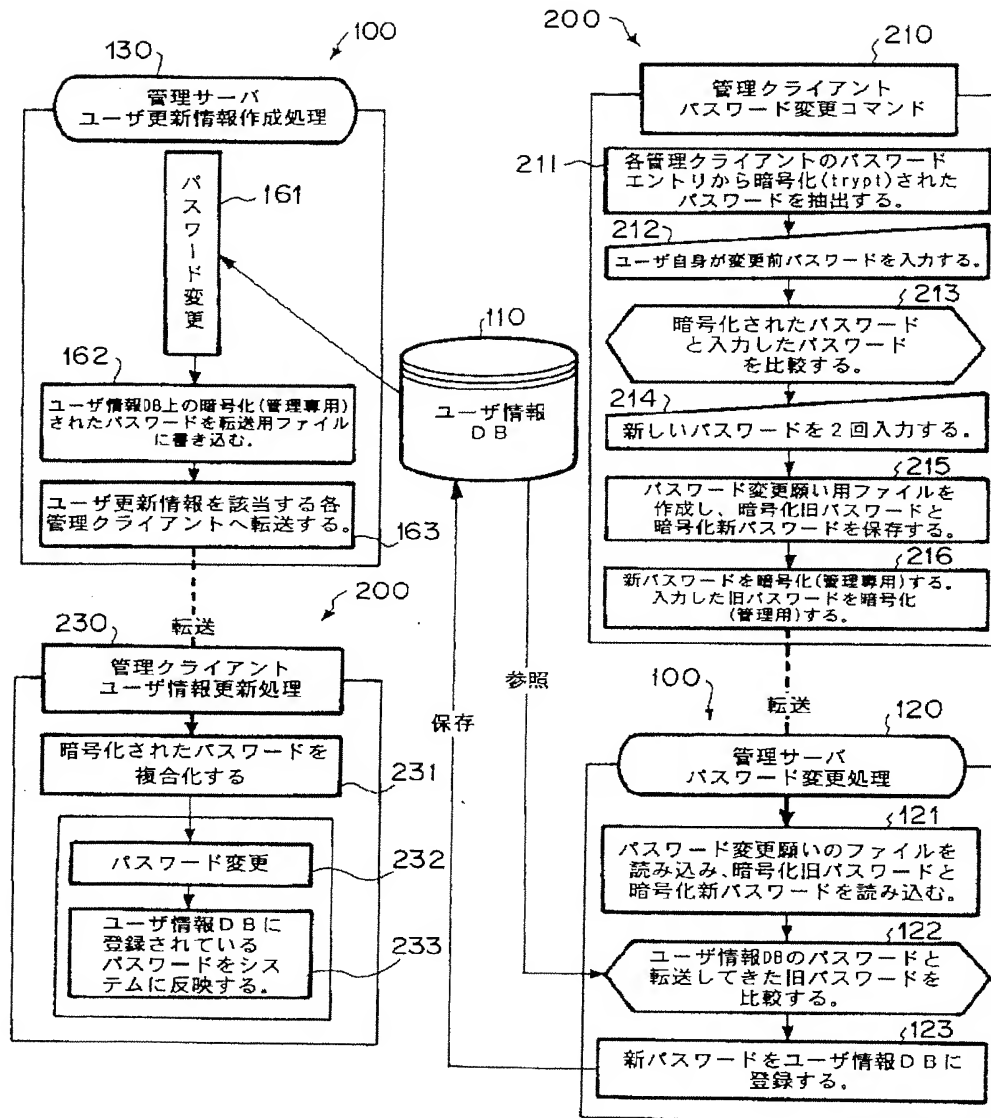
【図8】従来のネットワーク認証方法によるシステム概略図である。

【符号の説明】

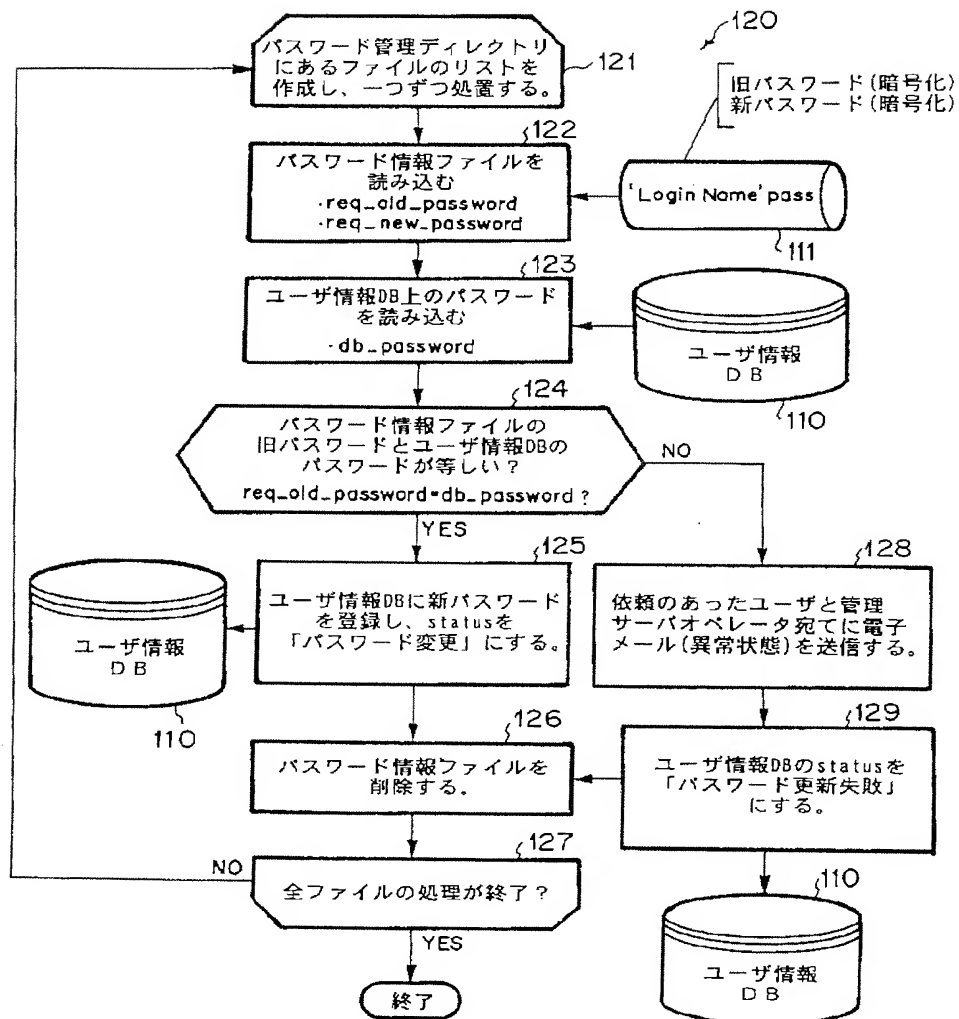
- 100 管理サーバ
- 110 ユーザ情報データベース
- 120 定時バッチパスワード変更処理
- 130 定時バッチパスワード処理
- 140 定時バッチ更新完了通知確認処理
- 200 管理クライアント
- 210 パスワード変更コマンド
- 220 定時バッチパスワード変更願い転送処理
- 230 定時バッチパスワード更新処理
- 240 更新完了通知確認



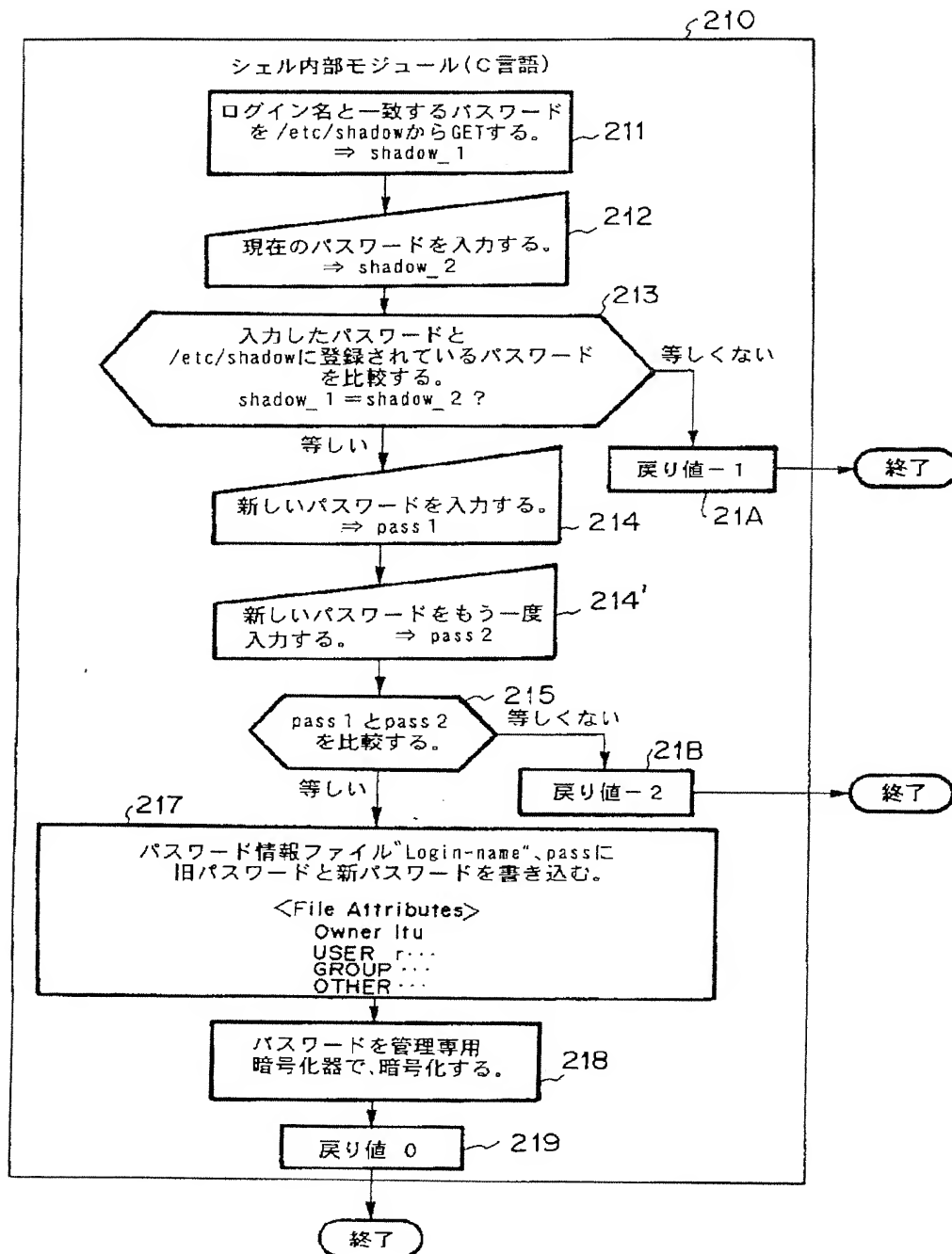
【図2】



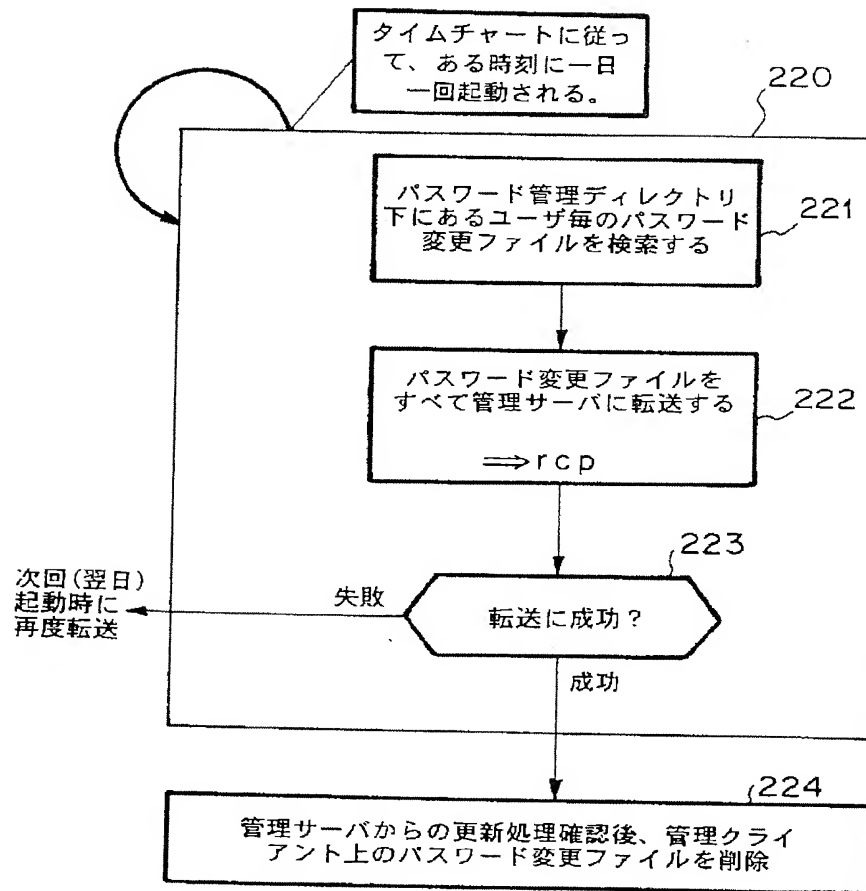
【図3】



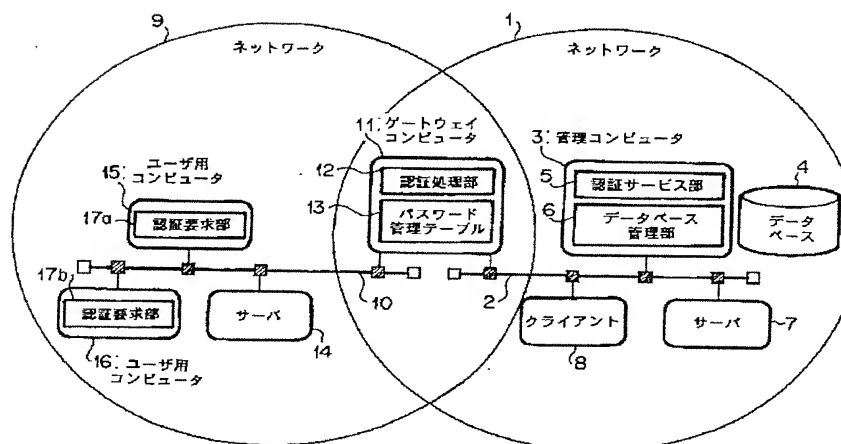
【図 4】



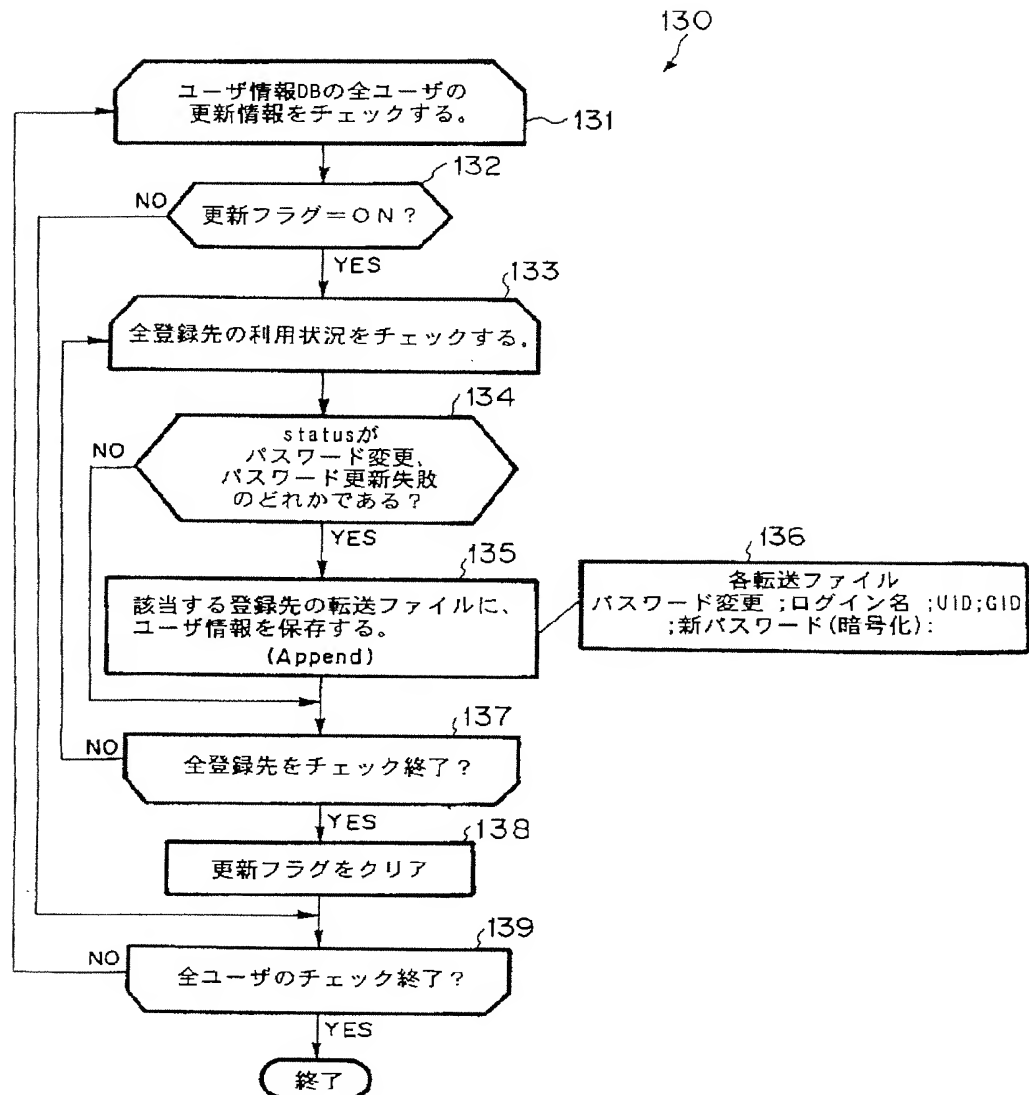
【図5】



【図8】



【図6】





【図7】

